Technology vs. Spam

Presentation to the
FCC Technological Advisory Council

Simson L. Garfinkel

MIT Computer Science and
Artificial Intelligence Laboratory

Friday, April 23, 2004

Rev 2

Spam is many things...

fax spam
Usenet Spam
Email spam
Pager spam

}

- ✓ Can be sent in bulk
- ✓ Cheap to send
- ✓ Cheap to receive & process 1 message
  (expensive to receive & process 1 million)
- ✓ No prior relationship between sender & receiver
- ✓ Jurisdictional arbitrage

Legislative Solutions:

- ✓ Hard to implement; hard to change
- ✓ Spammers have a seat at the table
- ✓ Don't extend internationally
- ✓ Don't seem to work

Technical Solutions:

- ✓ Fixed cost to implement and test
- ✓ Ideally require little user education or regulatory enforcement.
- ✓ Don't seem to work for long — easy for spammers to evolve new strategies

Weblog Spam

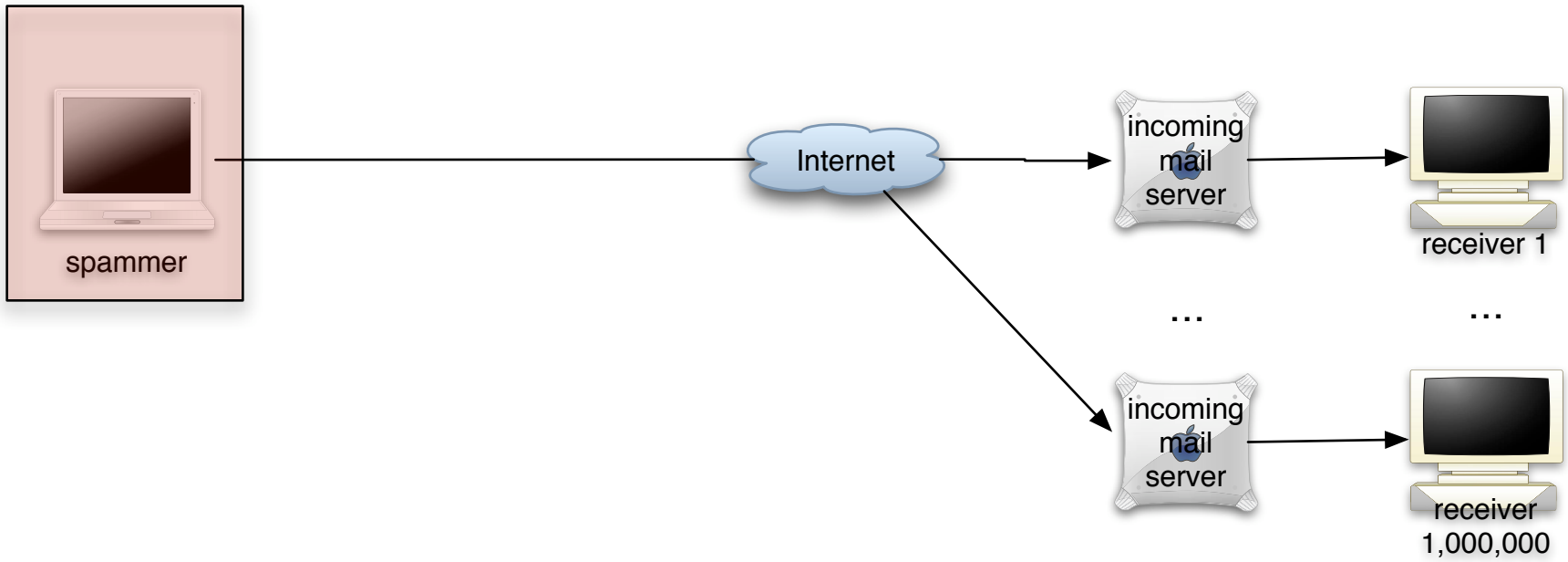
A new comment has been posted on your blog Simson's Weblog, on entry #3 (Adriaan Tijsseling).
http://www.simson.net/blog/archives/000003.php

IP Address: 213.91.217.13
Name: wellbutrin
Email Address: top@tredgf.com
URL: http://www.i-wellbutrin.com/

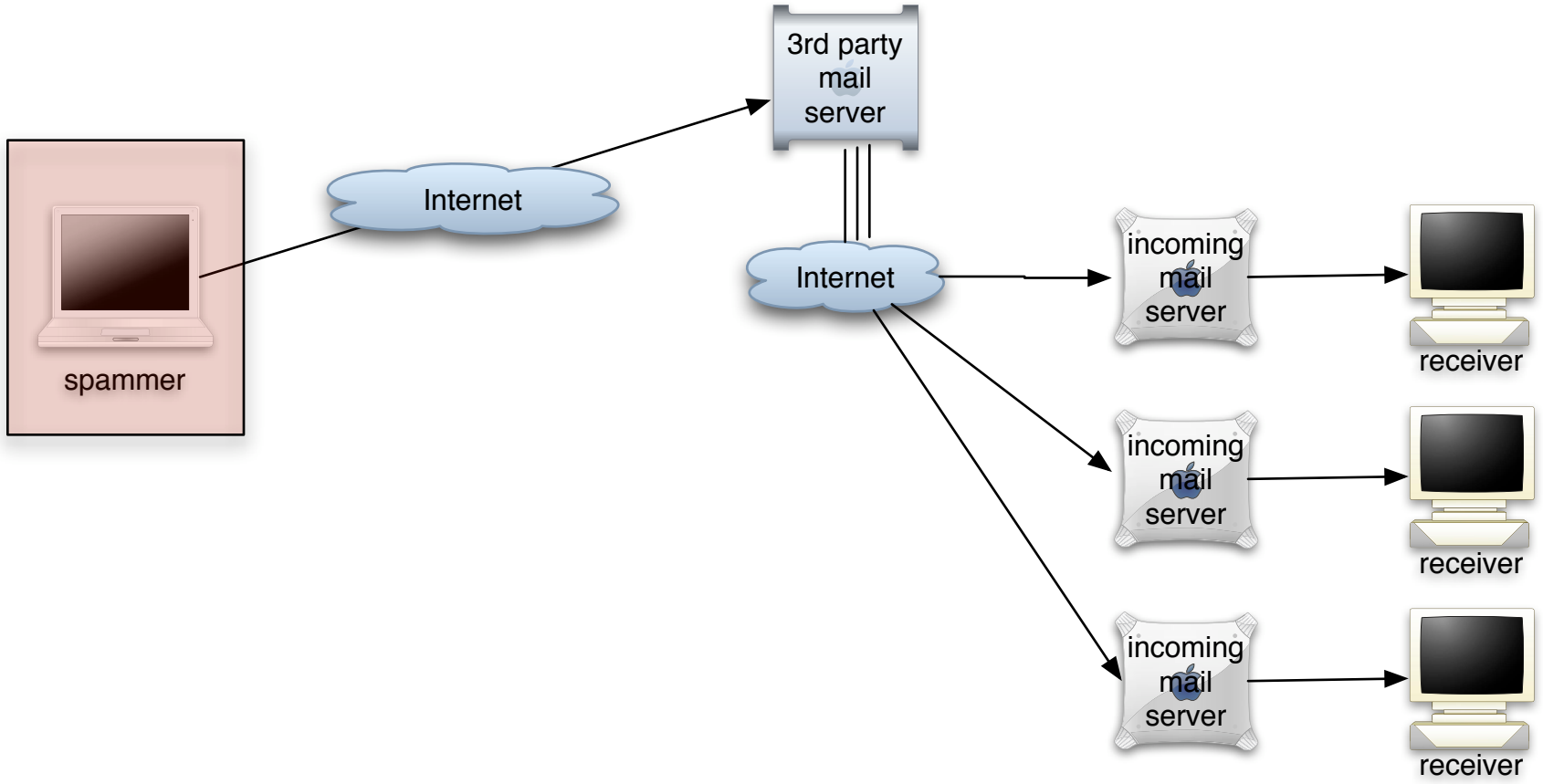
Comments:

Online Wellbutrin, wellbutrin, wellbutrin XL, wellbutrin SR is prescribed for the treatment of depression, but it is not for everyone. If you take cheap WELLBUTRIN XL, there is a risk of seizure, which is increased in patients with certain medical problems or in patients taking certain medicines. Buy Wellbutrin XL Now or visit this site: http://www.i-wellbutrin.com!

Evolution of email spam technology



simple spamming



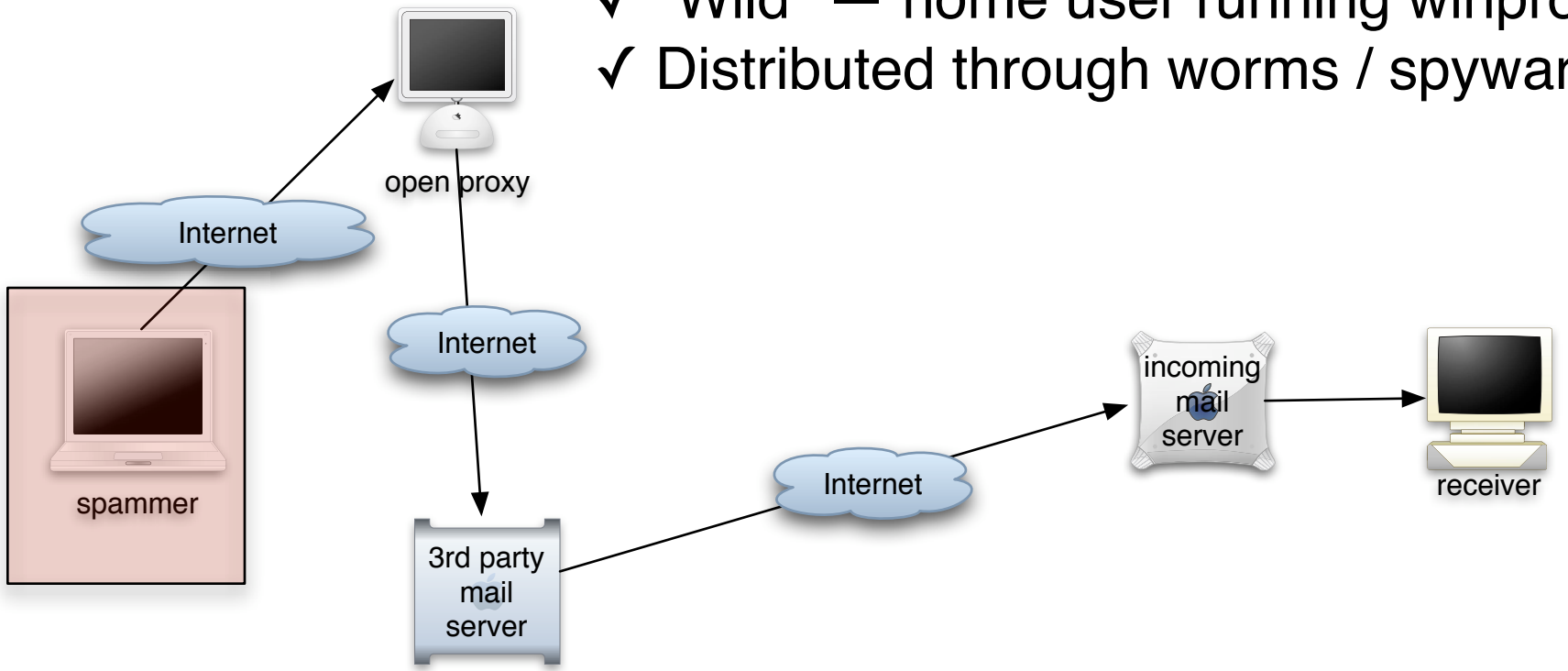
spamming through an open relay

(looks a lot like sending out mail to a mailing list)

Proxies can be:

✓ "Wild" — home user running winproxy

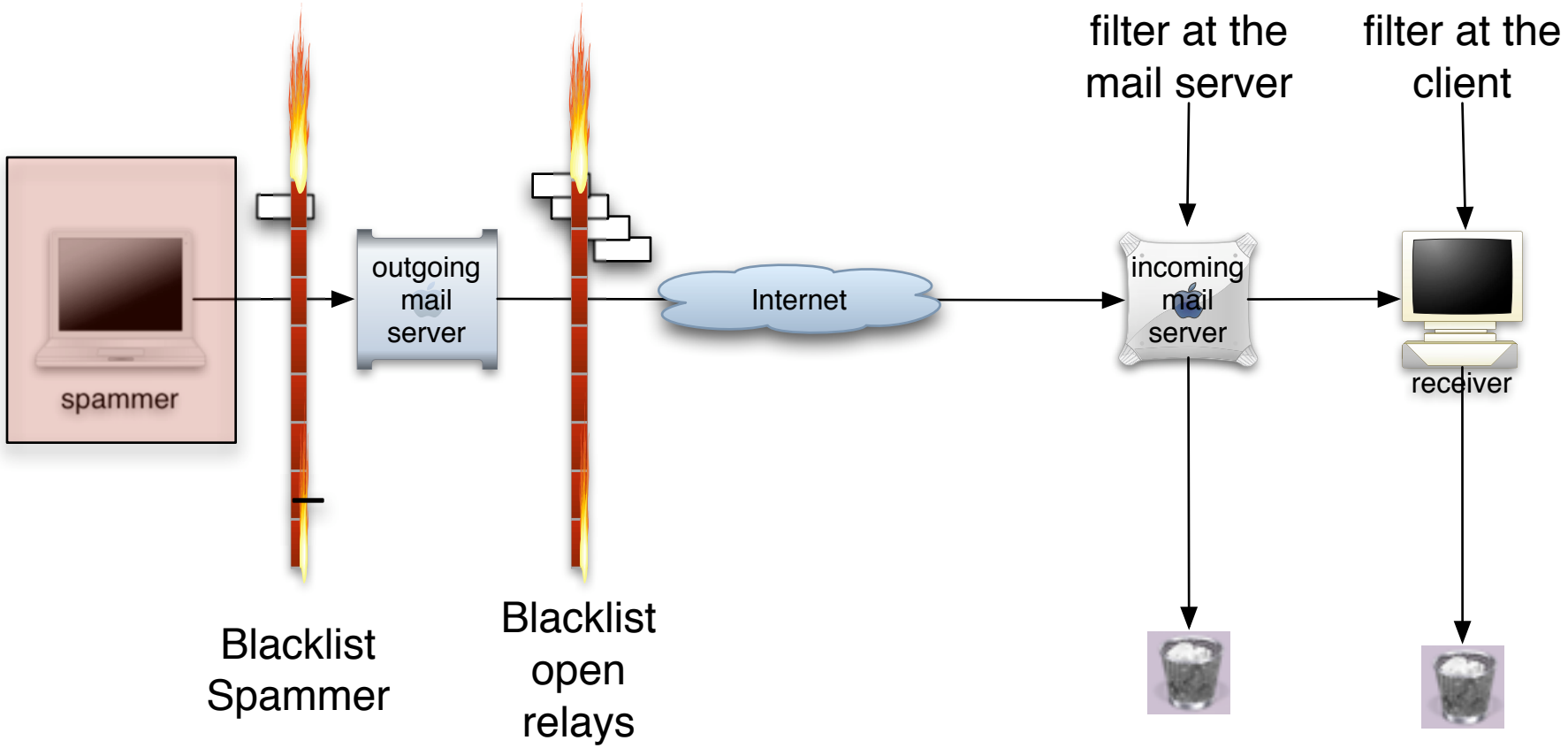
✓ Distributed through worms / spyware



open proxy + open relay

(makes tracing nearly impossible; most proxies don't keep logs)

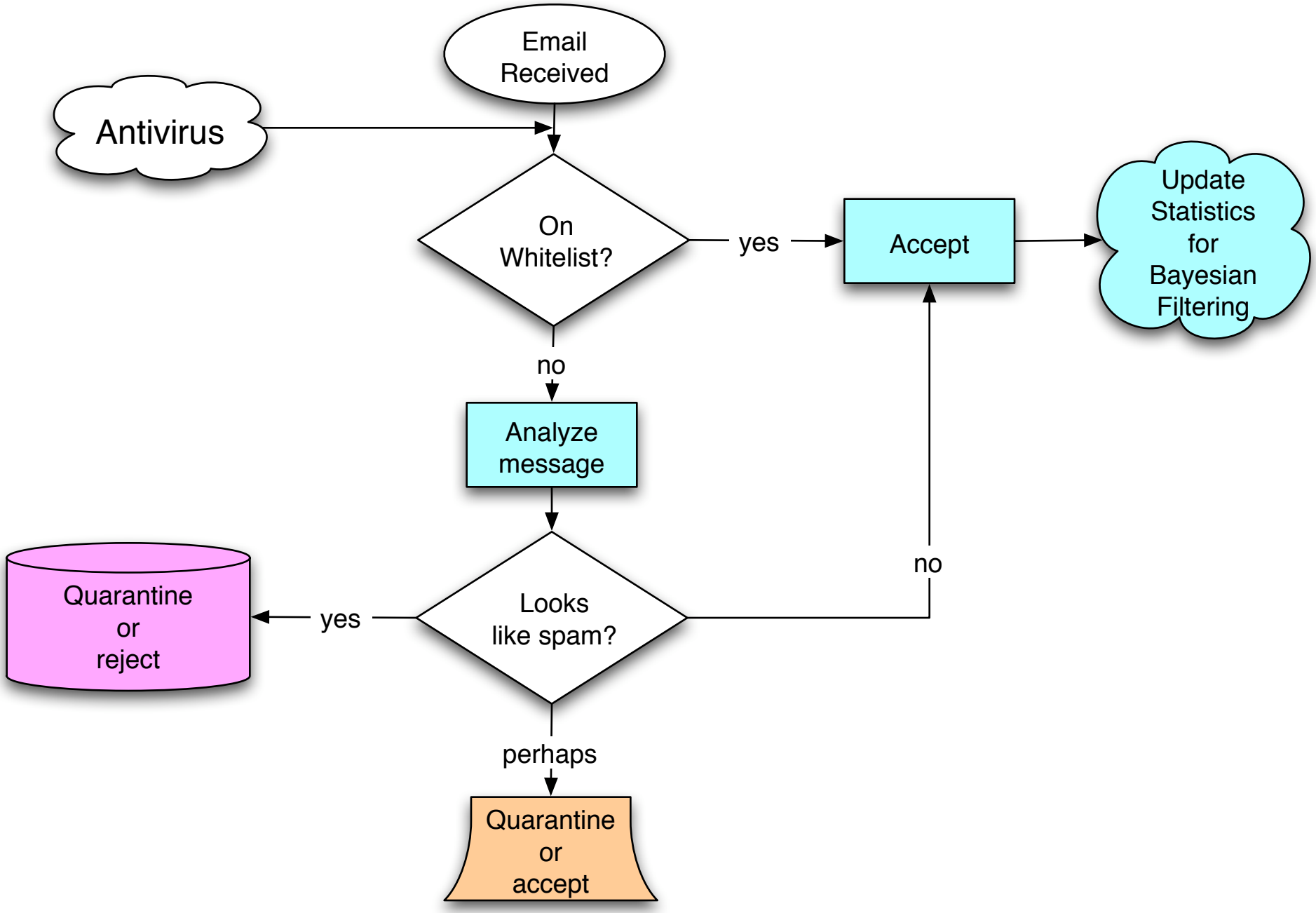
places for filtering spam:



Blacklist enforcement techniques:

- ✓BGP "black hole"
- ✓Distribute blacklisted IP addresses through DNS
- ✓Distribute blacklisted domain names through DNS

incoming mail rules:



ways for verifying whitelist:

From: address

From: simsong@acm.org

"Simson L. Garfinkel"

From: Name

Digital Signature

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

This is a message that was signed with GPG!
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.4 (SunOS)

iD8DBQFAZfuejRyogeMjJoIRArP5AKCHTCIFHJ8e0pPCtKEoitDsCtKEdwCdF3Dz
j8f+2Ob5pYVEMmUewtCSQOY=
=tiWt
-----END PGP SIGNATURE-----
```

ways for creating the whitelist:

Click "Reply" to have your message delivered

Email challenge/response

Computational postage (CPU cycles)

pq=2015993900449

"Electronic" postage ($$)
(Paypal; Peppercoin)

$.01 → simsong@acm.org

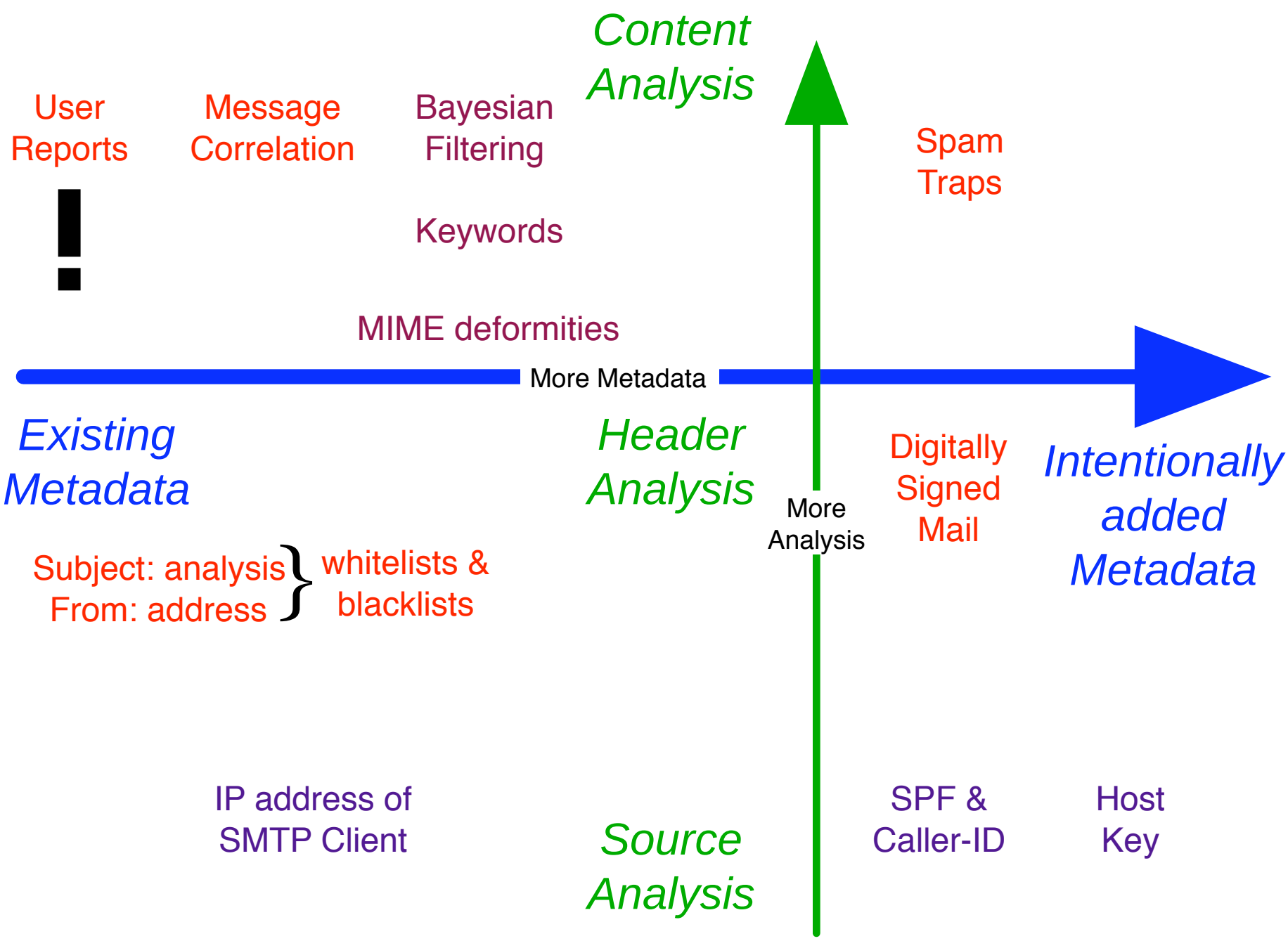
Reverse Turing Tests
(CAPTCHAs or Vision Tests)

hotmail

(Blind people hate them!)
(ADA Issues)

CMU Demo

All of these methods: easy for the sender to do one,
hard for the sender to do a million
(reversing the spam economics)


Not on whitelist?
spam identification techniques:
Content Analysis
User Reports
Message Correlation
Bayesian Filtering
Keywords
Spam Traps
!
MIME deformities
More Metadata
Existing Metadata
Header Analysis
Digitally Signed Mail
Intentionally added Metadata
More Analysis
Subject: analysis
From: address
whitelists & blacklists
IP address of SMTP Client
Source Analysis
SPF & Caller-ID
Host Key

fundamental problems with spam identification:

Spam can be arbitrarily
close to legitimate mail

One person's legitimate mail
is another person's spam

Prognosis: Content analysis is
ultimately a losing game

What about Outlaw Action?

Legitimate {mail | machines}
can be hijacked

(steal computational postage; steal micropayments; steal legit email)

Bayes is not the answer...

Idea sounds good: "spam" mail does not look like regular mail:

From: 4brad@templetons.com
Subject: EFF seeks CTO, I seek start-up team members, Blog, Awards, Foresight
Date: April 20, 2004 1:52:54 AM EDT
To: social-list@templetons.com

Hello members of my social mailing list. Here's my first message that some might class as spam because it contains a commercial element.
Since my definition of spam requires it be from a stranger, I would not class it that way, but as always, if you want out of my list, mail me.

Many things in this message:
o) The EFF is seeking a Technology Director, a sort of CTO. Is it your dream job? Direct and evangelize on technology and policy.

o) More about my new phone venture, and a call for team members.

Pr("Hello","members")
Pr("members","of")
Pr("of","my")
Pr("my","social")

From: fzhy81it@comcast.net
Subject: No Study, No Book No Interview, Get Ur Dip1oma & Degree Here drowze
Date: April 18, 2004 3:26:12 AM EDT
To: sascha@ex.com
Reply-To: fzhy81it@comcast.net

no degree = no job = no money
get an instant university degree = higher salary
** at least 2x times of ur current salary

no required tests, classes, books, or interviews!
get a Bachelors, Masters, MBA, and Doctorate (P-h-D) cert!

ALL CERTS ARE GENUINE & REAL WHICH IT CAN BE FOUND IN UNIVERSITY RECORD

--> call 1-917-591-5075 (24hrs on ca11)

Pr("no","degree")
Pr("degree","=")
Pr("=","no")
Pr("no","job")
...

Bayes is not the answer...

But spam can be arbitrarily close to real mail...

From: dagb@lopezclub.com
Subject: Simsong look at my google search lol kBgdH
Date: April 12, 2004 12:41:44 PM EDT
To: simsong@acm.org

I've heard all about Simsong,

Miracles only come around ohh so often, but we got one for you its called V i a g r a.. Impotency is a serious matter and should be threated seriously, so let us do it.. spice your love life now and buy the the GREATEST shop on the net.

http://www.pimpinprices.com/

Mucaale kabotu,
"Boost F. Gameness"

Aboriginal community leader Lyle Munro said anger in the community unsullied by any need to apply contemporary artistic licence. A police officer had his own pistol held against his stomach last Thursday that set agents to looking at BALCO also aren't detailed. The city has pinned its hopes of invigorating the entire if tied into the bar, what you'll be drinking.

Bayes is not the answer...

Real mail can be arbitrarily close to spam...

From: amoorse@glenmartinassociates.com
Subject: Position announcement -- Computer security
Date: April 20, 2004 2:26:35 PM EDT
To: slg@ex.com

Simson --

I met with a few folks at the NY State University at Albany yesterday. They're developing a new center for information security that will mix education and research missions.

I doubt you'll be interested -- the position is here in Albany -- but if you know anyone who might be, please pass on the following announcement.

The new *Center for Information Forensics & Assurance* (CIFA) is looking for a Director. The position announcement can be found at http://hr.albany.edu/sponsor/vacancy/R04-22.htm

Please circulate this announcement to anyone who might be interested in the position, or know of potential candidates.

More information about CIFA can be found at http://www.albany.edu/cifa/

Alan

What about "legitimate" spam?

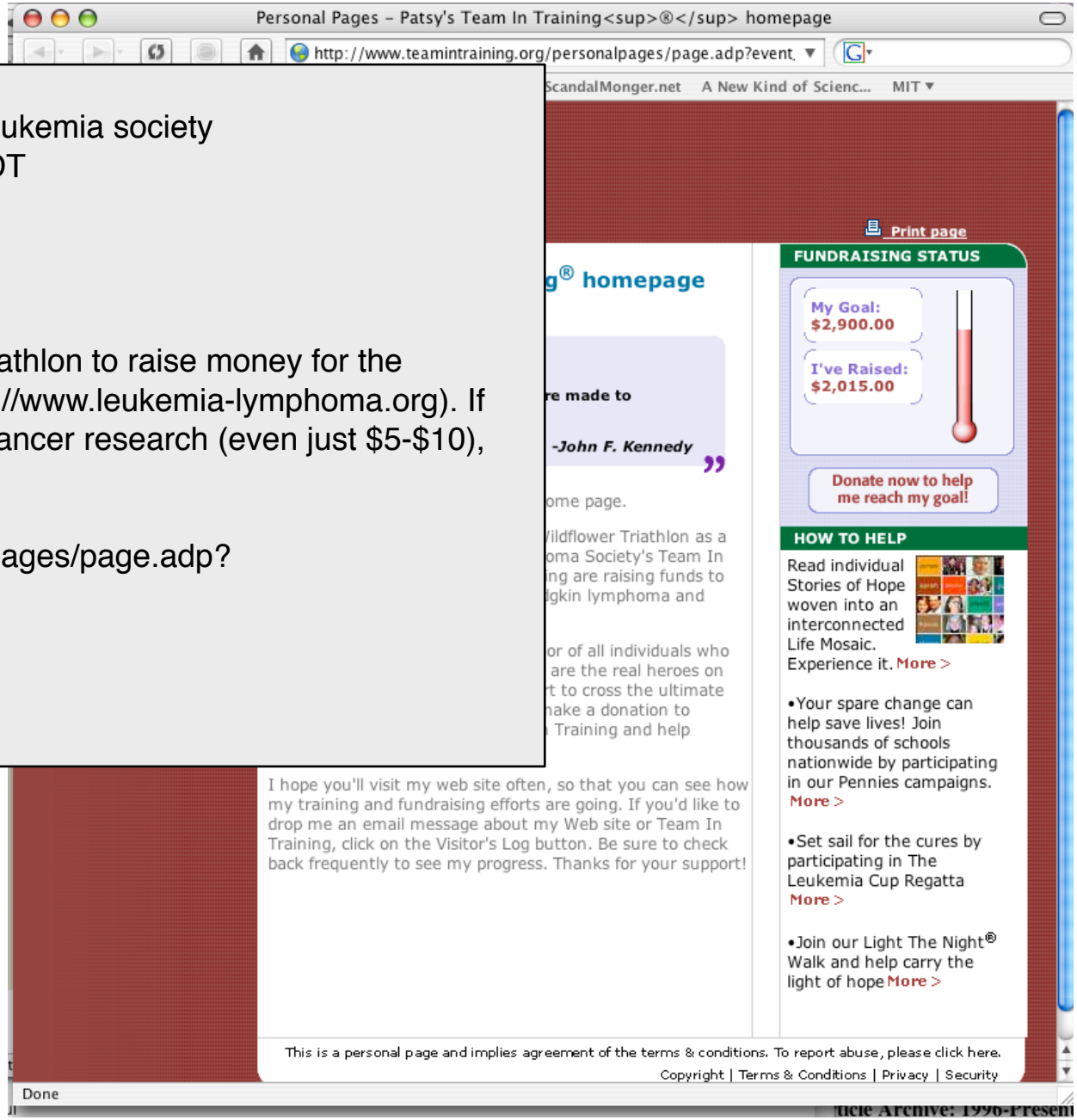
From: green@graphics.csail.mit.edu
Subject: A friendly solicitation for the Leukemia society
Date: April 20, 2004 10:28:33 AM EDT
To: csail-discuss@csail.mit.edu
Cc: vgn@csail.mit.edu

A good friend of mine is training for a triathlon to raise money for the Leukemia and Lymphoma Society (http://www.leukemia-lymphoma.org). If you'd like to donate money to support cancer research (even just $5-$10), you can here:

http://www.teamintraining.org/personalpages/page.adp?event_id=186554&user_id=164115

thanks,

Paul



"Bayes poison"

From: MWQASICI@mail2Maggie.com
Subject: **How are you?**
Date: April 19, 2004 7:51:25 AM EDT
To: simsong@acm.org
Cc: sitzman@acm.org, sjadelson@acm.org, skolhar@acm.org

drawbridge supremacy dinah distributive synge arteriole bombard laborious contralateral yonkers transpacific keats chordal alfalfa auction carnal laue dub clout

From: bxphu@rossbreeders.com
Subject: **NoRisk SimpleForm**
Date: April 13, 2004 4:50:43 AM EDT
To: slg@ex.com
Reply-To: bxphu@rossbreeders.com

<!--
ethanol b's coma klystron slight elmira mobil inroad operable censure edwina coil doubtful allay cruddy algebra taxonomy waxen ossify incense sextuplet arachnid calcutta antiquity castro delhi dingo ash persecute faa aperture eucharist observatory rockbound exorcism bessemer apparent shown slog determinate stooge sulk kinetic currant buddhist anglophobia centaur misogyny bran yarmulke anastomotic chester europa nomadic
!-->

From: Ri@sunmail1.com
Subject: **Fantastic News 21517**
Date: April 12, 2004 1:51:06 AM EDT
To: sandstrm@vineyard.net

"Top Only Store": http://www.perfectrxpalace.com?rid=1000

Visit now! - http://www.valuedrxnet.com?rid=1000

I hope you will enjoy this crazy tip of mine

zltmutywdcbmfctqiazhnscqxidisyftjbgfwgdbieoogheqhfzwybmxjsgdqnxcofhmllourekalqsuwssuverfyzkpnjtdoascngyhmihxyztwtlqpr,
wqlghaqaegcyiqggzsogpphklbveqoooebulcknirqgbimihgynvnuhzxefpsvdzwymykaidqohycpfinufdqmeosjdlehmchydtylzocg,
exvpmpupgjvwdgzomiaprbsnzfmqhuemraddpzvxiqtmxvcjffaxgsmhaaxhucvneyqvynvigowflborirqqlcxlcvtyzolfpdaprvxxmwczxssfjixxmuiqrbos,
bxjfaywxvvltzlqtdxdouccrktiojbilarqapoamllgkywdcwisskujxnulzxtmxmcabsanfntpmsuqq,
iipesouoztlufigjkhdkxiyqzmktcaymjqqdemrgfccmmjxxsajpkjijvsfzvfnevgjcsakaemmsvmpqmzhxirigmnfhtvnqbwutyevcr

poison+message

Despite all this, I don't currently have a spam problem